Amendments to the Specification:

Please delete the paragraph that begins on page 1, line 14, and replace as follows:

Various Personal e-Wallet and Data Vault products and services provide the ability to store, and sometimes share, personal information. Often, tools are provided, usually as a browser plug-in, to allow users to drag and drop from their stored data onto web forms while browsing. In some cases the web site's privacy policy is compared to the consumer's policy preferences and warnings are issued when there is a mismatch. Privacy policies are often based on the Platform for Privacy Preferences or P3P standard ~~(http://www.w3.org/TR/P3P)~~. Examples of such products include Microsoft's Internet Explorer and Passport service, Novell's digitalMe, Lumeria's SuperProfile and ZeroKnowledge's Freedom. Microsoft's Hailstorm service is an extension to its Passport service that provides data subject's a repository to store their personal data, and allows the data subject to grant permission to third party services and applications to access that data. The data subject has to give explicit access to third parties to access the data, and limited amount of privacy control is provided in that the data subject can specify who can access the data, for what purpose and revoke access or give access for a limited period of time.

Please delete the paragraph that begins on page 2, line 15, and replace as follows:

Current Personal Policy Enforcing products are designed to support a user's privacy policy preferences. A few of the e-wallet/data vault products provide some of this functionality, but the products listed here focus on allowing a complex privacy policy to

be represented and checked against either a web site's privacy policy or a data requester's privacy policy. These products use a P3P Preference Exchange Language or APPEL ~~(http://www.w3.org/TR/P3P-preferences)~~ as a language to express what P3P policies are acceptable. Agents retrieve the P3P policies associated with a web site and compare them to the APPEL rules. Mismatches result in warnings to the user. The user then takes whatever action they deem appropriate, such as not filling out the web site form. Examples of these agents are the AT&T Privacy Minder and the IBM Privacy Assistant.

Please delete the paragraph that begins on page 3, line 19, and replace as follows:

Standards have also been developed that promote the exchange of data over the internet as well as through non-internet messaging systems. The Customer Profile Exchange Specification or CPExchange ~~(http://www.cpexchange.org/standard/)~~ is a standard that defines how a P3P policy can be associated with personal data in an XML message. This policy applies to the data being provided by one party to another, and provides a way for an enterprise to include the applicable privacy policy with personal data exchanged between applications or between organizations.

Please delete the paragraph that begins on page 4, line 14, and replace as follows:

One major limitation is that current products assume that a data subject owns all personal data and/or all this data is available in one central repository or enterprise. However, a data subject's personal data is distributed across many enterprises and

repositories, and it is not practical to expect all this data to be collected in one central repository, or to be owned by one enterprise or even the data subject. Each enterprise owns some of the personal data they generate about a data subject, such as financial information in a bank, or health information in a hospital. Thus, a data subject's financial data may be held/owned by several enterprises such as his bank, credit card providers and broker, while his employment data is held by his employer and his health information is held by his doctors and health insurance providers. At the same time, the data subject has various other personal data, such as current phone numbers, addresses, clothing preferences, and a wide range of other preferences. None of the current products deal with allowing a data subject to express privacy preferences for controlling access to their personal data that is distributed across multiple enterprises and repositories. While enterprises often offer ~~data subjects~~ data subjects an "opt-out" policy by which the data subject can explicitly choose to allow or disallow the enterprise from sharing his data, this is an extremely limiting kind of privacy control since it imposes the policy of the enterprise on the data subject, with little or no capability to express policies specific to each data subject (other than the opt-out/opt-in option to some portion of the enterprise's policy). However, data subjects ~~wants~~ want complete freedom to specify their own privacy preferences (and not the data owner's or data holder's) on how their personal data is handled, regardless of where that data is stored or who owns that data.